

Know Your Customer “KYC” Voip Dialing, Inc.

December 20, 2024

Voip Dialing, Inc. Know Your Customer Policy and Procedures

Last Updated: 12/20/2024

Voip Dialing, Inc. has committed to maintaining robust processes for Know Your Customer (“KYC”) review to identify customer entities effectively and to prevent and mitigate fraudulent and illegal activity. The following policies and procedures (“KYC Policy”) have been adopted and are effective as of today.

Know Your Customer Policy Compliance Designation and Duties

All employees are responsible for acting in accordance with KYC Policy. The following individual(s) and team(s) have particular responsibility for upholding KYC Policy:

Ben Navon is the company’s KYC Compliance Lead and is fully responsible for the company’s KYC Policy and programs. The duties of the KYC Compliance Lead include overseeing policy implementation and updates, monitoring policy compliance, and employee training.

The KYC Compliance Lead will manage KYC Policy adherence in coordination with its teams and individuals.

Responsibilities:

- Perform pre-agreement reviews of all prospective customers to determine whether they meet company KYC Policy requirements, keeping detailed documentation of all information considered, decisions reached, and the individuals involved in the review.
- Perform escalated enhanced due diligence reviews and make KYC decisions for higher-risk clients identified in the standard review process.
- Responsible for ensuring that company KYC Policy sufficiently meets any applicable legal obligations while adequately addressing legal risks. Will consult with internal teams on legal questions that arise as part of KYC processes.
- Responsible for supporting the development or implementation of the tools, systems, or vendor resources needed to perform and document KYC processes in a timely and scalable manner.

Pre-Activation Requirements

Verified Identity Program

We collect the following data from each customer and validate against authoritative sources for accuracy where available.

- Full legal name
- State/Province/Country of Business Incorporation
- Employer Identification Number (EIN) or equivalent international tax ID
- Physical address representing a real place of business associated with the entity**
- Entity's parent company(ies) legal name(s) (if applicable)
- Entity's parent company(ies) state/province/country of business incorporation (if applicable)
- Entity's website(s)
- Name(s) of all individuals with 10% or more direct or indirect ownership of the entity
- Collection and validation of a contact email address with a domain name that exactly matches the entity website provided or a domain verified as controlled by the entity.
 - Care should be taken to detect impersonation attempts using similar domain names or email account takeover

**For US-based communications services, customers must provide a physical address in the United States. This must not be a virtual address, shared office location without a dedicated suite or floor, PO box, mail forwarding service, hosted server location, etc. An employee will view the address in Google street view to verify.

Where apply, we are requesting and qualifying additional details such as industry-specific license information or Legal Entity Identifiers (LEIs) to enhance the KYC review of entity identity.

Understanding Intended Use & History

KYC Policy requires an understanding of customers' intended use of services. The following materials must be collected and reviewed prior to service activation.

All customers:

- A description of the intended use of services
- Entity's website and public-facing materials¹

¹ Legal entity customers must have an active, dedicated web domain that meaningfully describes the nature of the entity's business and services. The entity's webpage and social media will also be used to assess reasonable business establishment (are there significant broken links, placeholder text, etc.), company leadership details, stated office locations, any published policies or processes, etc.

- The full set of products and services that will be enabled upon activation
- A certification of whether the entity or its owners have been subject to any prior enforcements or judgments for alleged illegal activity related to itself or related entities and, if so, provide details
- An active review of potentially negative reputational material including law enforcement actions, regulatory sanctions, or civil judgments

Additional details for Communicating End Entity (“CEE”)² customers:

- A description of the calls to be made
- A description of consent collection practices
- A description of legal compliance practices, including Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, and Fair Debt Collection Practices Act (if applicable)

Additional details for Communication Service Provider (“CSP”)³ customers:

- Active Robocall Mitigation Database information including entity’s FCC Registration Number (FRN) and Robocall Mitigation Database (RMD) ID
- FCC Form 499 Filer ID Number (if available)
- Confirmation of whether the CSP supports CEE customers (legal entity or consumer), CSP customers, or both, and how the CSP proactively verifies or controls for CEE vs. CSP customer categorization.
- The CSP’s signup and KYC processes
- Products and services marketed/offered

All data or communication collected and reviewed as part of verifying the identity or understanding the intended use and history must be documented and preserved in internal records such that future reviewers can determine what was reviewed or verified, any conclusions drawn, and the individual(s) that conducted the review.

Proactive Establishment of CEE vs. CSP Categorization

CEE and CSP customers represent different potential risks and regulatory considerations, and it is critically important to understand the nature of the customer’s business. Many businesses may have incorporated communications services into their own offerings despite not self-identifying as a CSP.

As part of its KYC Policy, Voip Dialing, Inc. will proactively evaluate whether a customer appears to be operating as a CSP or a CEE. While customer-provided information may be taken into account, KYC teams will not rely on a customer’s own designation of whether it is a CSP or CEE.

² Communicating end entities (“CEEs”) - A legal entity whose employees directly initiate or receive communications. CEEs include both entities initiating communications on their own behalf and Business Process Outsourcing companies

³ Communications service providers (“CSPs”) - A legal entity whose products or services enable other businesses to initiate or receive communications.

Team members will review the information provided by the prospective customer as well as its website and public materials to confirm if it appears to be a CSP.

Enhanced Due Diligence

For any entities that are part of potentially [high-risk categories](#) or that have identified [red flags](#) (as described in the Appendix of this document), additional steps must be taken to review, monitor, and restrict accounts. Accounts in this category will require approval by Ben Navon (“KYC Leader”). The KYC Leader will confirm whether a customer can be approved. If so, the KYC Leader will determine additional required risk mitigation measures which may include but are not limited to:

Additional customer activity monitoring, volume/capacity/spend limitations, restricting access to higher-risk products or services, penalty fees or agreement terms, KYC Leader approval for account changes, and as may be added from time to time.

The results of Enhanced Due Diligence will be fully documented and preserved to ensure the results are captured and any risk mitigation measures will be appropriately applied to the customer account.

Post Activation

Activity Monitoring

All customer accounts will be monitored for potentially unusual or suspicious usage. The following metrics will be monitored:

- Traceback requests
- Reports of alleged improper communications sent to the CSP from downstream CSPs, the general public, or others
- Federal Communications Commission and Federal Trade Commission consumer complaint data
- Call traffic statistics
 - Short call duration percentage
 - Average call duration
 - Answer Seizure Ratio (ASR)
 - Percentage of call attempts blocked due to improper caller ID (invalid, unallocated, on a DNO list)
- Requests for high capacity (calls per second or concurrent calls), particularly if disproportionate to the size of the account

Additional considered items monitored are payment status/history, customer sentiment, etc. The above is listed in roughly suggested order of importance but relevance depends on the services provided. For example, a Telephone Number provider will receive/recognize the majority of

complaints tied to the specific Telephone Number. CSPs used for outbound calls only and not phone number/inbound services must rely more heavily on traceback requests, call traffic statistics, and disproportionate capacity requests. Note, improper spoofing of valid caller IDs can make it difficult to monitor usage.

Further KYC Reviews

Customer accounts will be reviewed under the KYC Policy on an ongoing basis. Reviews will be inserted throughout the customer lifecycle as follows:

Detail how and when customer accounts will be reviewed on an ongoing basis. Such, ongoing reviews may include:

- Approval gates - Required approval for changes to business information or access to specific higher-risk products, high capacity, nonstandard use, etc.
- Triggered reviews - Thresholds and/or alerts for use, changes in use, disproportionate complaints, account changes, etc.
- Reporting - Global monitoring of customer activity; and
- Scheduled Reviews - Reconfirming account information and reviewing activity on a regular, scheduled basis. This will be performed based on the calendar year (quarterly, annually, etc.) and/or during a contract renewal cycle.

Appendix

Trial Accounts

Customers will not be given access to communications to/from the larger phone network without first undergoing a full KYC review and approval. All trial accounts will be time restricted and deactivated after 30 days, with any extension or requiring approval by KYC Leader(s).

To gain access to a trial account, customers must undergo either a full KYC review or, at a minimum, the collection, review, and approval of the following:

- Full legal name
- State/Province/Country of Business Incorporation
- Physical address representing a real place of business associated with the entity
- Entity's website(s)
- Entity contact name for trial account
- Collection and validation of a contact email address with a domain name that exactly matches the entity website provided or a domain verified as controlled by the entity

We limit the usage of trial accounts to ensure customers are not given access to/from the larger phone network without a full KYC review by:

- Trial access will be entirely closed off such that users are unable to make or receive communications to/from any phone numbers outside of the specific pool of internal phone numbers designated for testing in a closed environment.

And/or

- Customers in a trial access environment must validate their ownership over an external phone number via two factor authentication. Communication will only be possible between the closed test environment and the validated phone number.

Trial account usage will be closely monitored to ensure that 1) accounts are properly reviewed prior to activation and promptly deactivated upon expiration of the trial period, and 2) that trial account usage is not unreasonable, unexpected, abusive, or fraudulent. Should inappropriate use be found, offending trial accounts will be terminated immediately.

Criteria Prompting Enhanced Due Diligence

High Risk Categories

Accounts associated with the following industries or business models have a higher risk of carrying highly regulated, unsolicited, or potentially illegal communications. While many legitimate operators may be in these categories, many have been subject to enforcement actions. Customers

in these categories or who serve businesses in these categories require a higher standard of KYC review.⁴

- Affiliate marketing/lead generation⁵
- High-risk financial services (payday loans, debt relief, credit repair, auto/home warranties, loan offers by non-direct lenders, etc.)
- Third-party debt collections
- Political communications, fundraising (political or nonprofit), surveys
- IT support call centers not directly staffed and operated by the device or software manufacturer
- Highly marketed services (solar power, for-profit colleges, etc.)
- Businesses seeking US-based communications services that have a physical location in the United States but whose headquarters, staff, or leadership are located primarily outside of the United States.

Red Flags

The following behaviors should be considered red flags and prompt enhanced due diligence or potential rejection of the account.

- Unwillingness or expressions of hardship to provide requested information (or an unexpected eagerness to provide information)
- Aggressive, hostile behavior or over-escalation
- Claiming very large amounts of traffic with no clear basis (very few employees, brand new business entity, no web presence outside of a company website, etc.)
- Vague or incomplete answers to questions
- Unsolicited, notable interest in specific KYC processes and criteria
- Creating pressure to complete an agreement as soon as possible
- Customer's business entity is associated with a large number of related businesses or a complex structure of ownership without a clear reason
- Communication using email domains associated with multiple businesses or using public email domains (Gmail, Hotmail, etc.)
- Provided information, website, or documentation is unclear, incomplete, unprofessional, or appears to have been created very recently
- Customer is unwilling to speak over the phone or repeatedly avoids, cancels, or postpones meetings
- Customer presents as operating in one location but all customer contacts and operations seem to be located elsewhere or contacts claim to be traveling elsewhere

⁴ In some cases, communications may not be illegal even if they were unsolicited by the recipient.

⁵ Affiliate marketing or lead generation companies create, aggregate, or supply sales leads for other businesses. These companies may collect and sell lead data, make outbound communications to qualify and transfer "hot" leads or solicit clicks on affiliate SMS links, or solicit an inbound or scheduled phone call (often via SMS or email) with the purpose of transferring the caller to a third-party partner.